

Flanders Nieuwsflash Bulletin brengt maandelijks een overzicht van de artikels die verschenen zijn op onze website. Dit document is aangemaakt in een groter lettertype zodat het desgewenst kan afgedrukt worden als A5-boekje. Bezoek onze website voor de meest recente artikels.

www.flanderscomputerclub.be

FREEWARE – 26/08/2025

HOU JE PC SCHOON MET WISE DISK CLEANER

Merk je dat je computer trager wordt of dat je schijf bijna vol raakt, dan is het een goed moment om je systeem eens grondig op te schonen. Gelukkig hoeft je daarvoor geen technisch wonder te zijn. Met het gratis programma **Wise Disk Cleaner** kan je eenvoudig en veilig je computer opruimen en daardoor sneller laten werken.



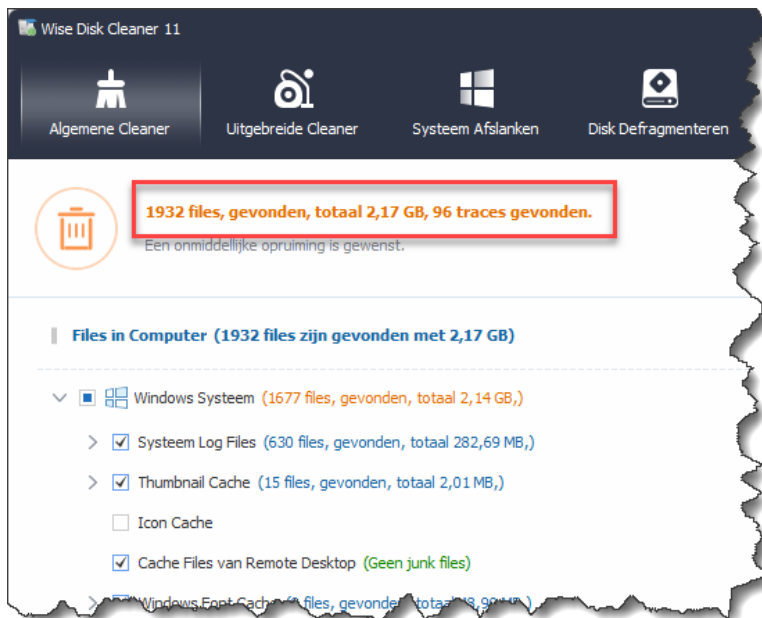
Het programma Wise Disk Cleaner is speciaal ontworpen als hulp bij het verwijderen van tijdelijke bestanden, logboeken, cache en andere digitale rommel die zich in de loop van de tijd ophoopt. Het programma maakt niet alleen schijfruimte vrij, maar zorgt er ook voor dat je computer soepeler blijft draaien. Werk je nog met een traditionele harde schijf dan biedt het programma ook de mogelijkheid om je harde schijf te defragmenteren. Let op: deze functie kan je best niet gebruiken voor SSD's.

Wise Disk Cleaner wordt beschouwd als een veilig programma, zolang je het installeert via de officiële website.

Het installeren van Wise Disk Cleaner is eenvoudig. Je downloadt het programma, opent het installatiebestand en volg de nodige stappen. Tijdens de installatie kan je voor de Nederlandse taal kiezen en eventuele extra software-voorstellen uitschakelen. Binnen enkele minuten is alles klaar voor gebruik.

Na installatie kan je een eerste scan uitvoeren en rustig door de resultaten bladeren. Je ziet dan precies welke bestanden als veilig beschouwd worden om te verwijderen, zoals tijdelijke internetbestanden of de inhoud van de prullenbak. De standaardinstellingen zijn zo gekozen dat je alleen overbodige bestanden verwijdert. Wil je liever dat bepaalde onderdelen

behouden blijven, zoals browsergeschiedenis of cookies, dan kan je die eenvoudig uitschakelen voordat je het opruimproces start. Zo hou je zelf de controle.



Het is ook mogelijk om automatische opschoningen in te plannen (*bijvoorbeeld wekelijks of maandelijks*) zodat je computer netjes blijft zonder dat je eraan hoeft te denken.

Kortom, Wise Disk Cleaner is een handig, veilig en gebruiksvriendelijk programma. Ideaal voor wie zijn computer fris en vlot wil houden, zonder ingewikkelde instellingen of technische kennis.

In onze programmabibliotheek vind je het programma samen met de nodige info.

U kan het programma ook zelf downloaden via onderstaande link.

<https://www.wisecleaner.com/wise-disk-cleaner.html>

FVG

AI (Hardware) – 13/08/2025

AI EN DE TOEKOMST VAN ONZE TOESTELLEN

Als we Microsoft mogen geloven dan zouden we over vijf jaar geen gebruik meer maken van een toetsenbord.

David Weston (*Vice President Enterprise & Security*) schetste deze week in een toekomstvisie hoe Windows er in 2030 zou moeten uitzien. Hij opent zijn visie met de opvallende uitspraak dat traditionele inputmethodes zoals toetsenbord en muis in de nabije toekomst overbodig zullen worden. Door artificiële intelligentie, zal onze manier van werken fundamenteel gaan veranderen. In een video op YouTube laat Weston ons zien hoe AI-agenten ons zullen bijstaan als digitale assistenten.

Die uitspraak valt niet bij iedereen in goede aarde. Heel wat gebruikers zeggen dat ze liever naar Linux of macOS overstappen dan hun muis en toetsenbord op te geven met het statement: **AI is handig, maar niet als het alles overneemt!**

Toch is het niet allemaal toekomstmuziek. Weston toont in zijn video ook hoe Microsoft nu al investeert in veilige, gebruiksvriendelijke systemen. Denk aan het **Windows Resilience Initiative**, een systeem dat computers in de toekomst op afstand moet kunnen herstellen, ideaal voor bedrijven. Weston is ervan overtuigd dat AI in de toekomst voor Microsoft en voor Windows een grote rol kan spelen, maar Microsoft moet vooral fouten voorkomen en werken natuurlijker maken.



Maar niet alleen onze pc heeft te maken met de vernieuwingen die via AI tot stand komen. We kunnen ons bijvoorbeeld geen leven meer voorstellen zonder mobieltje. En die mobiele telefoons zullen vast nog wel een aantal jaren alom tegenwoordig zijn, maar ook hier vormt AI een stevige bedreiging. De opkomst van Google's AI Mode (*en vergelijkbare AI-chatbots*), kan op termijn het einde betekenen van de smartphone zoals we die nu kennen. Schermen worden minder belangrijk, want als AI steeds slimmer en spraakgestuurd wordt, dan is het typen van zoekopdrachten of het eindeloos scrollen overbodig. In plaats van via een scherm gebruik je straks vooral je stem en wellicht gebaren.

Grote namen als voormalig Apple-designer Jony Ive werken samen met OpenAI nu al aan nieuwe apparaten zonder klassiek scherm, maar met een microfoon en camera. Ze reageren direct, zijn waarschijnlijk superdraagbaar (*zoals een ketting of pin*), ze zien wat wij zien en ze beantwoorden je vragen in een natuurlijke taal.

Waar we nu nog steeds uren naar ons mobieltje turen, voorspellen experts dat dit over een paar jaar ouderwets zal aanvoelen, net zoals faxen of cd's nu.

De tijd zal dit alles echter moeten uitwijzen.

De video van David Weston kan je hier bekijken:

<https://www.youtube.com/watch?v=ccpXNBsTaGk>

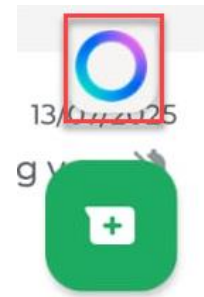
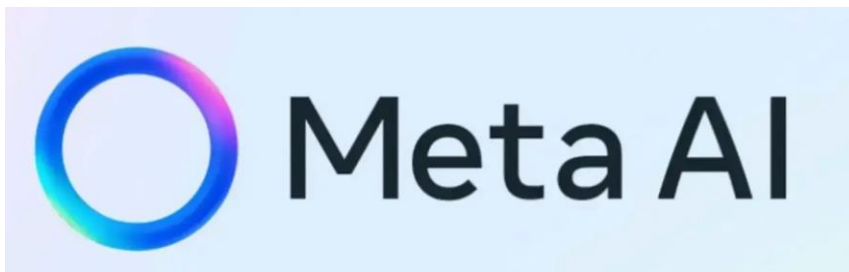
FVG

(Geraadpleegde bronnen: welingelichtekringen.nl, Clickx)

SOCIALMEDIA – 04/08/2025

STORENDE WHATSAPP META-AI KNOP

Sinds kort is er in WhatsApp een extra knop verschenen waarmee gebruikers de artificieel intelligente chatbot Meta AI kunnen gebruiken in de app. De knop met een blauwpaarse cirkel is plots rechtsonder verschenen.



Als ik de commentaren op diverse internet forums mag geloven dan zijn er maar heel weinig mensen gediend van deze nieuwe optie, vooral omdat er geen mogelijkheid is om ze uit te schakelen.

Meta AI is een gratis chatbot die werkt op basis van artificiële intelligentie (AI) en is dus vergelijkbaar met het populaire ChatGPT. Je kan met deze nieuwe knop allerlei vragen laten beantwoorden.

Voorlopig is Meta AI enkel beschikbaar in de mobiele apps op Android- en iOS-telefoons. De knop is dus niet te zien in de desktopversie van WhatsApp. Volgens WhatsApp-ontwikkelaar Meta voldoet de optie aan de privacyregels van de Europese Unie (EU). Meta AI kan enkel lezen wat je naar de chatbot stuurt, zodat die je vragen kan beantwoorden. Alle andere informatie blijft versleuteld, zo benadrukt de technologiegigant.

Zoals we reeds vermeldde is er geen instelling om de knop te verwijderen.

Volgens commentaren op de verschillende forums zou dit illegaal zijn, omdat Meta spreekt over een optionele functie.

Laten we hopen dat de verwijder-mogelijkheid niet te lang op zich laat wachten.

FVG

BEVEILIGING - 27/07/2025 **CYBERCRIMINALITEIT**

Cybercriminaliteit is iets waar we meer en meer mee te maken krijgen. Zowel bedrijven als particulieren worden het slachtoffer. Cybercriminaliteit omvat een breed scala aan kwaadaardige activiteiten, zoals: E-mail- en internetfraude of identiteitsfraude, waarbij je persoonlijke gegevens worden gestolen en misbruikt.

De methoden die cybercriminelen gebruiken, variëren afhankelijk van hun doelen.



Laat ons eerst de belangrijkste vormen van cybercriminaliteit overlopen:

- **Phishing**
Dit is een methode waarbij criminelen valse berichten of e-mails sturen die eruit zien alsof ze van een betrouwbare bron komen, zoals een bank of een populaire website. Het doel is om gevoelige informatie van slachtoffers te verkrijgen, zoals wachtwoorden of creditcardgegevens.
- **Malware**
Malware is schadelijke software die op een computer of netwerk wordt geïnstalleerd om schade aan te richten of toegang te verkrijgen. Enkele veelvoorkomende vormen zijn virussen, wormen, Trojaanse paarden, ransomware en spyware. Ransomware is bijvoorbeeld een type malware dat bestanden vergrendelt die pas worden vrijgegeven na betaling van losgeld.
- **DDoS-aanvallen**
Bij een DDoS-aanval (*Distributed Denial of Service*) proberen cybercriminelen een website of een online dienst te overbelasten met een enorme hoeveelheid dataverkeer, zodat deze niet meer bereikbaar is voor gewone gebruikers.
- **Hacken**
Hackers gebruiken verschillende technieken om toegang te krijgen tot systemen, netwerken of computers zonder toestemming. Dit kan bijvoorbeeld gebeuren via zwakke wachtwoorden of kwetsbaarheden in software. Hackers doen dit voor verschillende redenen, maar meestal voor financieel gewin of politiek activisme.
- **Man-in-the-Middle (MitM) aanvallen**
Bij deze aanval onderschept de aanvaller communicatie tussen twee partijen (*zoals tussen een gebruiker en een website*) om gegevens te stelen, te wijzigen of zelfs valse informatie in te voeren.
- **Identiteitsdiefstal**
Cybercriminelen verkrijgen persoonlijke informatie van slachtoffers, bijvoorbeeld door phishing of het hacken van databanken en gebruiken deze informatie om frauduleuze handelingen uit te voeren, zoals het openen van bankrekeningen of het aanvragen van kredieten.
- **Social engineering**
Dit is een techniek waarbij cybercriminelen zich voordoen als iemand anders om mensen te manipuleren tot het onthullen van vertrouwelijke informatie. Dit kan bijvoorbeeld via telefoon, e-mail of zelfs via fysieke ontmoetingen.
- **SQL-injectie**
Hierbij maakt de aanvaller gebruik van kwetsbaarheden in databasesystemen om kwaadaardige code in een website of applicatie te injecteren, waardoor toegang tot gevoelige gegevens mogelijk is.
- **Botnets**
Dit zijn netwerken van geïnfecteerde computers die op afstand worden bestuurd door een cybercrimineel. Ze kunnen voor verschillende doeleinden worden gebruikt, zoals het uitvoeren van DDoS-aanvallen, het verzenden van spam e-mails of het stelen van gegevens.

Bescherming tegen cybercriminaliteit begint met waakzaamheid.



Dit zijn enkele effectieve manieren om jezelf te beveiligen:

- **Sterke wachtwoorden gebruiken**
Gebruik zoveel mogelijk lange wachtwoorden met een combinatie van letters, cijfers en speciale tekens. Probeer een uniek wachtwoord te gebruiken voor elke website. Overweeg hierbij het gebruik van een wachtwoordmanager, bijvoorbeeld **KeePass**.
- **Software up-to-date houden**
Zorg ervoor dat je besturingssysteem, applicaties en antivirusprogramma's regelmatig worden bijgewerkt. Updates bevatten vaak beveiligingspatches tegen nieuwe bedreigingen.
- **Wees voorzichtig met links en bijlagen**
Klik nooit zomaar op links en open geen bijlagen in e-mails van onbekende afzenders. Phishing-e-mails proberen vaak te misleiden door heel betrouwbaar te lijken.
- **Twee-factor-authenticatie (2FA) inschakelen**
Activeer 2FA voor je accounts. Dit voegt een extra beveiligingslaag toe door een tweede verificatiemethode, zoals een sms-code, toe te voegen.
- **Gebruik een beveiligde internetverbinding**
Vermijd openbare wifi-netwerken voor gevoelige transacties. Indien je zo'n gevoelige transactie toch moet uitvoeren op een openbaar (lees onbeveiligd) netwerk, gebruik dan een VPN (*Virtual Private Network*) programma.
- **Wees alert op verdachte activiteiten**
Controleer regelmatig je bankrekeningen en online accounts op ongewone transacties of activiteiten.
- **Back-ups maken**
Maak regelmatig een kopie van je belangrijke bestanden. Gebruik hiervoor een externe schijf of cloudopslag. Dit helpt je bij het herstellen na een eventuele ransomware-aanval of het verlies van gegevens.
- **Privacy-instellingen controleren**
Beperk de hoeveelheid persoonlijke informatie die je online deelt, en controleer de privacy-instellingen van je sociale media.

Elke methode heeft zijn specifieke voordelen en beperkingen, maar een gecombineerde aanpak (zoals het gebruik van sterke wachtwoorden, 2FA, en regelmatige updates) biedt de beste bescherming.

Ik kan ook aanraden om je in te schrijven bij de dienst **SafeOnWeb!**
SafeOnWeb is een app van het **Centrum voor Cybersecurity België** (CCB) met als hoofddoel burgers snel en accuraat te informeren en te adviseren over cyberbeveiliging, digitale dreigingen en online veiligheid.
De app kan je terugvinden in Google Play:
<https://play.google.com/store/search?q=safeonweb+app&c=apps>

*Dit artikel heeft nog een vervolg waarin we bespreken wat je als gebruiker moet doen wanneer je computer besmet is door één of andere malware.
U kan dit artikel en het vervolg terug vinden op onze website onder Publicaties → Diverse publicaties.*

FVG

FREEWARE – 10/07/2025

BESCHERM JE BESTANDEN IN DE CLOUD MET CRYPTOMATOR

Steeds meer mensen maken gebruik van cloudopslagdiensten zoals Dropbox, Google Drive en OneDrive om bestanden veilig te bewaren en gemakkelijk te delen.

Hoewel deze diensten je gegevens tijdens de verzending versleutelen, bieden ze niet standaard een **end-to-end encryptie**. Dit betekent dat anderen, inclusief de cloudaanbieder zelf, mogelijk toegang kunnen krijgen tot jouw gegevens.

Gelukkig is er een eenvoudige en betrouwbare oplossing: **Cryptomator**.



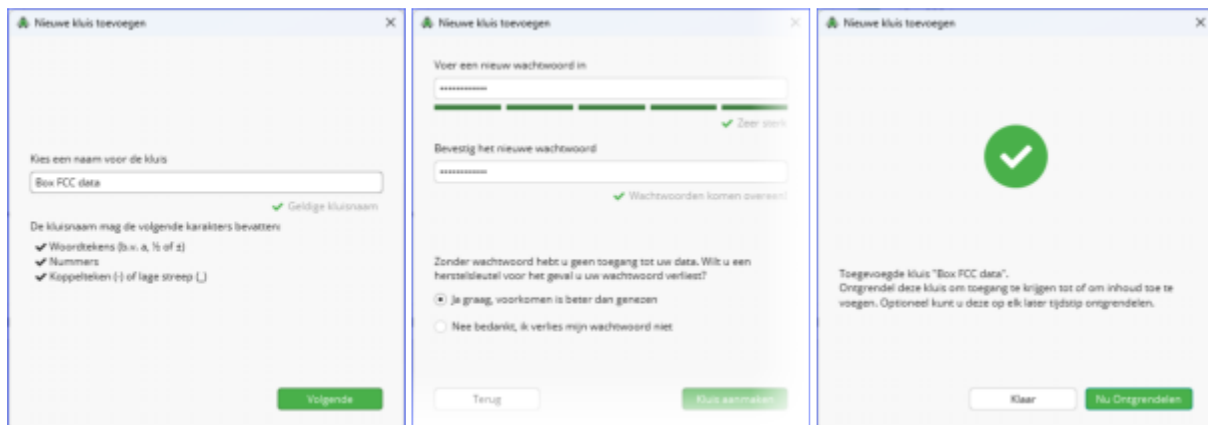
Cryptomator is een gratis en open-source programma waarmee je je bestanden versleutelt voordat je ze opslaat in de cloud. Het programma werkt als een digitale kluis op je computer of smartphone. Alles wat je erin zet, wordt automatisch beveiligd met sterke end-to-end-encryptie.

Cryptomator versleutelt niet alleen de inhoud van je bestanden, maar ook bestandsnamen en mappenstructuur.

Alleen jij kan de versleutelde bestanden openen met jouw wachtwoord.

En Cryptomator werkt naadloos samen met alle bestaande clouddiensten. Je hoeft dus niets te veranderen aan je manier van werken. Je voegt gewoon een extra beveiligingslaag toe.

Of je nu gevoelige documenten opslaat, persoonlijke foto's bewaart of zakelijke gegevens deelt, met Cryptomator heb je zelf de controle over je privacy. Zelfs als je cloudaccount wordt gehackt blijven je bestanden onleesbaar zonder het wachtwoord van je Cryptomator "kluis" (*vault*).



Cryptomator "kluizen" zijn eigenlijk beveiligde mappen op een locatie naar keuze. Die locatie zou bijvoorbeeld de synchronisatiemap van je cloudopslagdienst kunnen zijn, maar evengoed een gewone map. Voor elke kluis stel je een sterk wachtwoord in. Dit wachtwoord is de sleutel tot je versleutelde gegevens. Zonder dit wachtwoord zijn de bestanden onbruikbaar. Wanneer je de kluis ontgrendelt met je wachtwoord dan maakt Cryptomator hiervoor een virtuele schijf op je computer. Alles wat je naar deze virtuele schijf kopieert, wordt automatisch versleuteld voordat het naar de cloud wordt gesynchroniseerd. Wanneer je bestanden uit de kluis opent, worden ze automatisch ontsleuteld. Cryptomator gebruikt hiervoor de geavanceerde encryptiestandaard AES-256 met een sleutellengte van 256 bits, om een hoge mate van beveiliging te garanderen.

Kortom, Cryptomator is een tool die je de controle geeft over de beveiliging van je gevoelige gegevens in de cloud, door ze lokaal te versleutelen voordat ze ergens anders terechtkomen.

In onze programmabibliotheek vind je het programma samen met de nodige info.

U kan het programma ook zelf downloaden via onderstaande link.

<https://cryptomator.org/downloads/win/>

FVG

Secretariaat p/a Moretuslei 3 B-2180 Ekeren	Informatie Per post: via secretariaat Per telefoon: 0032 3 2895573 Per e-mail: info@flanderscomputerclub.be	Lidgelden 60 EUR voor 1 jaar IBAN: BE89 9734 5282 0585
Redactie: Frank Van Goolen		